BLOCKCHAIN: LA NUEVA ERA DE LA IDENTIFICACIÓN DIGITAL EN INTERNET

BLOCKCHAIN: THE NEW ERA OF DIGITAL IDENTIFICATION ON THE INTERNET

Javier Martínez Boada

Abogado
Investigador en formación
Universidad Camilo José Cela

Francisco José Santamaría Ramos

Profesor Ayudante Doctor
Universidad Complutense de Madrid

RESUMEN

Internet permite a las personas realizar en el ámbito digital prácticamente las mismas cosas que hacen en los entornos reales. En el mundo físico, las personas pueden ser identificadas a través de un documento único que contiene los datos esenciales que las individualizan frente a las restantes. Por el contrario, hoy por hoy en la esfera digital, los usuarios son capaces de tener bajo su control diferentes identidades que pueden identificarlos de manera fehaciente o no. Bajo esta situación, en los entornos digitales los usuarios pueden actuar desde el anonimato o pseudoanonimato con el fin de atentar contra la confianza en las transacciones y, en consecuencia, generar inseguridad jurídica. A la vista de tal situación, entidades como la UE han elaborado propuestas para crear carteras de identidad digital en las que se registren los datos de identificación de los usuarios. Sin embargo, no se presta la debida atención al hecho de que Internet es un espacio digital que no conoce fronteras y en el que difícilmente puede obligarse a los operadores del resto del mundo a hacer uso de una identidad digital única. En este contexto y dada la importancia de implantar un mecanismo de identidad digital única, aparece *blockchain*, un sistema trasnacional, inmutable, distribuido, seguro y descentralizado que puede ser opción idónea para instaurar una identidad digital única que permita identificar fehacientemente a los usuarios que operen en Internet. El objetivo de este artículo es analizar la situación actual de la identidad digital y argumentar que *blockchain* es un sistema idóneo para garantizar la identidad digital y facilitar la identificación en Internet.

PALABRAS CLAVE

Identidad digital, identificación, anonimato, Internet, *blockchain*.

ABSTRACT

The Internet allows people to do virtually the same things in the digital realm as they do in real enviroments. Within the physical world, every person can be identified by a unique document containing the essential data that individualizes them from everyone else. On the contrary, today in the digital sphere, users can have a multitude of different identities under their control that can reliably identify then or not. Thus, in digital environments, users can act anonymously or pseudo-anonymity to undermine trust in transactions and, consequently, producing legal uncertainty. In view of such a situation, entities such as the EU have drawn up proposals for the creation of digital identity wallets in wich users' identification data are recorded. However, due attention is not paid to the fact that the Internet is a digital space that knows no borders, and in wich it is difficult to force operators from the rest of the world to use a unique digital identity. In this context and given the importance of implementing a unique digital identity mechanism, blockchain appears as a transnational, immutable, distributed, secure and decentralized system that may be an ideal option to establish a unique digital identity that allows users operating on the Internet to be reliably identified. The objective of this article is to analyze the current situation of digital identity. We also argue that blockchain is a suitable system to ensure digital identity and facilitate the identification on the Internet.

KEYWORDS

Digital identity, ID, anonymity, Internet, Blockchain.

DOI: https://doi.org/10.36151/TD.2024.114

BLOCKCHAIN: LA NUEVA ERA DE LA IDENTIFICACIÓN DIGITAL EN INTERNET

Javier Martínez Boada
Abogado
Investigador en formación
Universidad Camilo José Cela

Francisco José Santamaría Ramos
Profesor Ayudante Doctor
Universidad Complutense de Madrid

1. INTRODUCCIÓN

Hasta hace poco, la sociedad gestionaba, procesaba y archivaba la información de una forma elemental, utilizando como soporte el papel. Sin embargo, el siglo XXI dio lugar a la digitalización y a la llegada de la denominada sociedad de la información (Santamaría Ramos, 2024: 38).

La aparición de la sociedad de la información la humanidad ha sido un punto de inflexión cuyas manifestaciones más relevantes son la digitalización y la irrupción de las llamadas tecnologías disruptivas[1].

En estas circunstancias, se han desarrollado espacios virtuales que hasta hace apenas unas décadas eran inimaginables. En ellos, las personas pueden realizar actuaciones similares a las que desarrollan en los entornos tradicionales.

En el mundo físico las personas cuentan con una única identidad[2] y una serie de datos que las diferencian del resto de individuos. Sin embargo, a la hora de acceder a los servicios de la sociedad de la información en los nuevos entornos virtuales los usuarios tienen la

posibilidad operar en multitud de plataformas utilizando diferentes identidades digitales (creadas por ellos mismos) que imposibilitan su trazabilidad y detección[3].

En contraste con lo que ocurre en los entornos reales —donde la identificación de las personas se lleva a cabo a través de documentos únicos como el DNI—, en el entorno digital los procedimientos de identificación electrónica están basados en datos alfanuméricos (por ejemplo, un usuario y una contraseña diseñados por el propio usuario). Esta información puede haber sido inventada por el usuario, de tal forma que ni el nombre de usuario ni los datos introducidos para crearlo correspondan con su identidad, es decir, puede actuar bajo diferentes seudónimos que hacen imposible su identificación. También es posible que la información utilizada por el usuario corresponda a otra persona y, de este modo, suplante su identidad (Batuecas Caletrío, 2022: 947).

A medida que la esfera digital se expande, cobra mayor importancia el tratamiento de los problemas que genera. En el ámbito de la identidad personal, el abordaje de algunos de estos inconvenientes puede incluso comportar la necesidad de replantear su configuración en el nuevo entorno. Cabe incluso concebir la posibilidad de que bajo el control de cada usuario exista una identidad digital y que ésta sea única, como ocurre en el mundo físico.

El modo de administrar la identidad digital en la red ha ido evolucionando de modo paralelo a las transformaciones que ha experimentado Internet, entre las que cabe destacar el incremento de la oferta de servicios que de un modo u otro afectan a la identidad personal. En la Web 1.0 los usuarios únicamente estaban capacitados para leer páginas y realizar comentarios en foros y blogs. Es decir, no podían interactuar de ninguna forma, por lo que su identidad se encontraba limitada. La Web 2.0 permite a los internautas introducir información para crear perfiles digitales y cada usuario es libre de conformar su identidad con los datos que decida incluir a la hora de crear su usuario. Además, la información y las cuentas de usuario están bajo control de los proveedores de servicios, que en cualquier momento pueden privar de identidad a los usuarios según sus propios criterios (Allen, 2016). Finalmente, la Web 3.0 se erige como un espacio de lectura, escritura y confianza que todavía se encuentra en desarrollo y se considera como el futuro de Internet. Se trata de un Internet descentralizado donde se distribuirá la información y los datos cuando los usuarios lo deseen y sin que ninguna entidad sea propietaria o gestione la información; esta posibilidad viene facilitada por determinadas tecnologías disruptivas, por ejemplo, *blockchain* (Gallardo Rodríguez, 2023: 1016).

Así como Internet revolucionó la forma en la que se compartía y se accedía a la información, la tecnología *blockchain* promete transformar de forma determinante la manera en la que se realizan las transacciones entre las personas físicas y jurídicas o, incluso, entre máquinas (Alvarado Bayo y Supo Calderón, 2021: 346).

La evolución tecnológica de los últimos años ha modificado nuestras vidas en multitud de aspectos. A medida que se ha explorado el potencial de la transformación digital se ha descubierto que la naturaleza segura, inmutable y descentralizada de *blockchain* tiene el potencial de superar los desafíos actuales y rediseñar la forma en la que se almacenan,

comparten, custodian y gestionan los datos de los usuarios (Albiol-Perarnau y Alarcón Belmonte, 2024: 2).

La tecnología *blockchain* comenzó a estructurarse como sistema de intercambio de activos digitales, especialmente del bitcoin, pero con el tiempo la evolución de este mecanismo ha propiciado la ampliación de sus funcionalidades, que pueden revolucionar la forma de actuar en la red (Corredor Higuera y Díaz Guzmán, 2018: 407). Una de ellas es su utilización como protocolo de identidad digital, es decir, como sistema de almacenaje de los datos de los usuarios que les permita identificarse dentro de Internet.

A la vista de las ventajas de *blockchain* a la hora de conformar una identidad única digital que permita identificar fehacientemente a los usuarios dentro de Internet, el Reglamento (UE) 2024/1183 del Parlamento Europeo y del Consejo, de 11 de abril de 2024, por el que se modifica el Reglamento (UE) n.º 910/2014 en lo que respecta al establecimiento del marco europeo de identidad digital (en adelante, eIDAS 2) regula una cartera de identidad digital europea que permitirá a los internautas almacenar, gestionar y controlar sus credenciales en los entornos virtuales (Flamini *et al.*, 2024: 1).

Es importante subrayar que Internet es un espacio que carece de fronteras y que los contenidos circulan entre países en cuestión de milésimas de segundos (Ruiloba Castilla, 2006: 56). Por esta razón, difícilmente puede regularse y crearse una cartera de identidad digital para un solo Estado o un conjunto de Estados como la UE, pues los internautas que no pertenezcan a estos continuarán navegando y actuarán en Internet con identidades no trazables y, en consecuencia, sin que se les pueda identificar.

Como se verá a lo largo de este artículo, para identificarse digitalmente los usuarios requieren de un protocolo internacional sencillo de usar y seguro que les permita administrar exclusivamente sus datos digitales en Internet e identificarse fehacientemente en los entornos virtuales para garantizar la confianza y la seguridad en las transacciones que se realizan en la red.

Bajo todos estos presupuestos, este estudio trabajo pretende, primeramente, estudiar las cuestiones de interés que plantea la identidad digital en la actualidad y analizar cómo están conformados los métodos de identificación. Una vez examinada la situación, se propondrá el uso de la tecnología *blockchain* como sistema de gestión de identidad digital y protocolo de identificación digital internacional. A tal efecto, se analizarán fuentes bibliográficas e informaciones de diversa procedencia que muestran en qué situación se encuentra la identidad digital de las personas, cómo se gestionan y regulan actualmente los datos de identidad digital de los usuarios y cómo *blockchain* puede servir para identificar digital y globalmente a los internautas.

2. LA IDENTIDAD DIGITAL

Desde el momento en el que una persona nace, adquiere personalidad jurídica y se encuentra amparada y protegida por el ordenamiento jurídico. Tal y como establece el artícu-

lo 50 de la Ley 20/2011, de 21 de julio, del Registro Civil, toda persona tiene derecho a un nombre —y, por lo tanto, a ser identificado por su nombre y sus apellidos—. En nombre constituye, además, una de las formas a través de las que los poderes públicos controlan la identidad de los individuos (Benavente Moreda, 2013).

Por su parte, la identidad de una persona[4] es el conjunto de rasgos propios que la definen como individuo y la diferencian del resto de sujetos que conforman la sociedad (Gete-Alonso y Calera, 2018: 35).

Este concepto es de vital importancia para el ser humano, puesto que es el que otorga la capacidad jurídica o, dicho de otro modo, la personalidad jurídica. En resumen, la identidad confiere la capacidad para ser sujeto de derecho (Santamaría Ramos, 2015: 39)[5].

Justamente es esta capacidad para ser sujeto de derecho la que se reconoce y protege como derecho fundamental dentro del artículo 6 de la Declaración Universal de los Derechos Humanos de 10 de diciembre de 1948. Este precepto dispone que todo ser humano tiene derecho a que se le reconozca en cualquier lugar su personalidad jurídica. De esta forma, la identidad, entendida como el conjunto de rasgos que caracterizan y distinguen a unas personas de otras y que le atribuyen su personalidad jurídica, es un derecho fundamental que debe ser reconocido con indepencia del lugar en el que actúe, es decir, tanto en el ámbito físico como en la esfera digital (Santamaría Ramos, 2015: 39)[6].

En el mundo real, la identidad se configura a partir de una serie de datos vinculados a la persona, entre ellos el nombre, los apellidos, la fecha de nacimiento, domicilio, número de identificación fiscal, etc., información que está contenida en su DNI, es decir, en su identificación a nivel nacional, o en su pasaporte, documento de identificación a nivel internacional (Merchán Murillo, 202: 185).

Como vemos, en un entorno físico, la identificación de una persona y la comprobación de su identidad como persona se lleva a cabo a través de ciertos instrumentos (por ejemplo, el DNI o el pasaporte) en los que aparezcan todos los datos que individualizan al sujeto frente a los restantes miembros de la sociedad. En cambio, en el entorno virtual, los usuarios se diferencian del resto en virtud de su identidad digital[7]. Esta puede ser definida como la expresión electrónica del conjunto de caracteres con los que una persona, ya sea física o jurídica, se individualiza frente a las demás (Fernández Burgueño, 2012: 127).

A la hora de determinar qué se entiende por identidad digital, algunos autores sostienen que este concepto alude exclusivamente a un conjunto limitado de datos, entre ellos el nombre y apellidos, los datos biométricos y el DNI. Otros, sin embargo, consideran que la identidad digital estará conformada por todos los datos que existan de una persona en de Internet, es decir, tanto los reconocidos de forma oficial (como el lugar de nacimiento, la fecha de nacimiento, la vecindad civil, la nacionalidad o el DNI) como los creados por el propio usuario (usuarios, avatares, ideologías, creencias, chats, etc.) (Batuecas Caletrío, 2022: 957)[8].

Como se ve, no existe consenso en la definición de identidad digital, pues, ya se ha dicho, algunos autores incluyen dentro de ella toda la información que existe en Internet sobre un sujeto, es decir, tanto los datos que hacen referencia a su identidad como la in-

formación que se refiere a su personalidad digital y, por ende, a su reputación digital. De acuerdo con lo expuesto, la identidad digital debe estar compuesta por los datos que sean únicamente consustanciales a la propia persona, es decir, los que hacen al usuario único y diferente dentro de la red (Batuecas Caletrío, 2022: 957).

Actualmente, las personas no poseen una identidad digital única que las diferencie fehacientemente de los demás usuarios dentro del amplio entorno de Internet, sino que cada proveedor de servicios, red social o web requiere diferentes datos personales, por ejemplo, usuarios, contraseñas, direcciones de correo electrónico, claves o datos de recuperación que conforman diversas identidades digitales de la persona para cada sitio web, red social o entorno virtual en cuestión (Ibáñez Jiménez, 2018: 322-323). De esta forma, puede asumirse como identidad digital desde el perfil que un usuario ha creado por sí mismo en la red social Facebook hasta el expediente electrónico en el que una entidad bancaria conserva actualizados los datos personales de cada uno de sus clientes (Fernández Burgueño, 2012: 127).

Junto a la amplitud de información existente para determinar la identidad digital de los internautas[9], dentro del ámbito virtual los usuarios también pueden tener intenciones maliciosas. Tal y como se encuentra conformado actualmente el espacio digital los usuarios pueden cometer el denominado «robo de la identidad digital», es decir, tienen la capacidad de hacerse pasar por otra persona bien accediendo al propio perfil del usuario que quieren suplantar, bien creando una cuenta utilizando los datos de identificación de dicha persona (Batuecas Caletrío, 2022: 952).

Asimismo, la identidad de las personas que actúan en Internet puede ser desconocida o de difícil determinación, ya que los usuarios pueden utilizar datos falsos o que dificulten la identificación (por ejemplo, nombres de usuario, direcciones de correo electrónico o *nicknames*) para registrarse en el espacio digital. Además, ni siquiera mediante la dirección IP puede identificarse al usuario, dado que este puede haberse accedido a la red a través de dispositivos electrónicos que no sean de su propiedad (Martínez Calvo, 2020: 158).

2.1. NORMATIVA APLICABLE A LA IDENTIDAD DIGITAL

Conviene enumerar brevemente las normas que el legislador ha ido aprobando para solventar estos problemas para que el lector pueda analizar rápidamente la legislación dedicada a la materia y observar en qué situación nos encontramos actualmente.

Dado que el ámbito digital no tiene fronteras y que la transmisión electrónica de datos no se circunscribe únicamente a un territorio determinado, la UE se encargó de elaborar diferentes textos normativos para ofrecer soluciones y contribuir a mejorar la identificación de los internautas (Merchán Murillo, 2022: 1389).

El primer cuerpo legal que hace breves referencia a la identificación de los usuarios en la red fue la actualmente derogada Directiva 1999/93/CE del Parlamento Europeo y del Consejo, de 13 de diciembre de 1999, por la que se establece un marco comunitario para la firma electrónica. La Directiva pretendía instituir un marco común en el que los Estados

miembros ajustaran su Derecho interno a una serie de condiciones sobre firma electrónica. Sin embargo, al transponerla a los ordenamientos jurídicos internos, los países miembros establecieron marcos jurídicos dispares que hacían imposible realizar transacciones electrónicas transfronterizas con confianza (Merchán Murillo, 2022: 1390).

En vista de este problema, se elaboró un segundo instrumento legal que derogó la Directiva 1999/93/CE. Hablamos del Reglamento (UE) n.º 910/2014 del Parlamento Europeo y del Consejo de 23 de julio de 2014 relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior y por la que se deroga la Directiva 1999/93/CE, en adelante eIDAS. Este Reglamento creó un marco normativo encargado de regular la identificación digital y los servicios de confianza dentro del territorio de la UE. En otras palabras, la norma consagró un marco jurídico común a todos los Estados miembros que establece los requisitos y las condiciones para identificar digitalmente a las personas físicas y jurídicas a través de medios de identificación electrónica (Alamillo, 2019: 9).

A título de ejemplo práctico, en España la identidad digital de una persona —y, por consiguiente, su identificación en el ámbito virtual— se obtiene a través de figuras como el DNI electrónico o los certificados electrónicos. Este tipo de instrumentos surgen con el objetivo de dar respuesta a la necesidad de conferir seguridad a las operaciones que se realizan a través de Internet y hacer posible que un usuario actúe con su identidad real. El DNI electrónico es único y no se puede falsificar. Está certificado por un tercero y, al igual que los certificados electrónicos, se utiliza principalmente para acceder a los procedimientos en la Administración pública en los que requieren este tipo de identificación. Por otro lado, el certificado digital, ya sea de persona física o jurídica, es un conjunto de datos asociados a una identidad avalada por un prestador de servicios de certificación y se instala dentro de los navegadores de los usuarios para identificarse al actuar frente a organismos públicos (Lucas Durán y García Martínez, 2019: 179).

Como puede verse, estas herramientas de identificación electrónica se utilizan en las relaciones de los individuos con el sector público. El eIDAS el que dota de libertad a los Estados miembros para que decidan si las implantan en del sector privado o no[10].

Finalmente, con el transcurso del tiempo, y a la vista de que el eIDAS dejaba cierta libertad a los Estados miembros para implantar estos mecanismos de identificación digital dentro del sector privado, surgió la idea de elaborar un espacio de confianza transfronterizo. A tal efecto, el 3 de junio de 2021 la Comisión Europea desarrolla la Propuesta[11] del eIDAS 2. Este nuevo Reglamento pretende colmar las lagunas que existen en el actual eIDAS y desarrollar una forma de identificación digital, a saber, una cartera de identidad digital europea que involucre también al ámbito privado (Merchán Murillo, 2022: 1400).

Por el momento, tan solo es una proposición que han realizado los organismos europeos. De acuerdo con la legislación vigente, puede afirmarse que garantizar la identidad digital en los espacios virtuales es, actualmente, un proceso complejo, a pesar de los mecanismos de los que disponemos actualmente para generar propiedades digitales identitarias,

asociarlas a un usuario concreto y autentificarlas mediante recursos biométricos, tarjetas digitales, certificados electrónicos etc. (Benach y Pueyo, 2013: 75).

Como se ha adelantado, Internet es una herramienta que no conoce de fronteras, es decir, que tiene alcance global (Salvador García, 2024: 82). De esta forma, la implantación de una identidad única destinada a los internautas pertenecientes a los Estados miembros de la UE se enfrenta a un problema añadido: ¿Qué sucede con aquellos usuarios pertenecientes a otros territorios que no son parte de la UE?

Hace años que nos encontramos inmersos en un contexto mundial que reclama la creación de un Derecho global llamado a ordenar las relaciones de acuerdo con criterios de justicia (López-Medel Báscones, 2024: 28). De esta forma, se hace necesaria la elaboración de una regulación internacional de la identidad digital individualizada para cada sujeto en de Internet, pues, como se ha dicho, cualquier persona desde cualquier parte del mundo puede actuar en la red.

Como se ha visto, tal y como se encuentran constituidos los entornos digitales, los internautas pueden crearse perfiles introduciendo datos creados por ellos mismos que no son confiables, pues con ellos no se puede averiguar la identidad digital que «*anda detrás*» de ese usuario o cuenta. Para solucionarlo, resulta más necesario que nunca la creación de una identidad única y universal que sirva de base para imputar derechos y obligaciones y conocer qué sujeto en concreto está actuando en el entorno virtual (Lucas Durán y García Martínez, 2019: 178).

Dado que actualmente no disponemos de una identidad digital única, los usuarios pueden llevar a cabo actuaciones en la red contrarias a la legislación, cometer delitos o realizar actuaciones para las que no poseen capacidad legal. Un ejemplo es el libre acceso de los menores a contenidos a los que, según su edad, no tendrían que acceder. Hablamos de los contenidos pornográficos[12]. A través de una identidad digital única se garantizaría que la persona que navega por Internet puede ser identificada; es decir, es quien dice ser, puede probarlo y puede demostrar su capacidad de obrar, edad o libertad de actuación (Merchán Murillo, 2022: 1388)[13].

Por el momento, las personas que navegan a través de Internet e interactúan en los entornos virtuales pueden poseer múltiples identidades, utilizar identidades de terceros a través de la suplantación de identidad o participar en actuaciones electrónicas para las que no tienen capacidad legal (por ejemplo, acceder a contenidos pornográficos, comprar[14] productos a través de Internet o registrarse[15] en redes sociales en las que no cumplen la edad mínima de inscripción).

En resumen, parece evidente la necesidad de que exista una identidad digital única por cada usuario que opere en la red. En este sentido, seguidamente se analizan algunos aspectos cruciales en la materia: el sistema actual de garantía de la identidad digital, la verificación de la identidad real de los internautas y las razones que hacen necesaria la implementación de una identidad digital única, individual e internacional para cada usuario.

3. SISTEMA ACTUAL DE GARANTÍA DE IDENTIDAD DIGITAL

Con el propósito de situar al lector en el escenario actual, es preciso analizar la evolución de los sistemas de identificación digital con el fin de conocer la modalidad ante la que nos encontramos y el esquema hacia el que nos conduce el desarrollo tecnológico y la realidad actual.

Primeramente, como sistema inicial de identidad digital, hay que destacar el modelo de identidad centralizada-jerarquizada. En él, las identidades digitales dependen de cada sitio web o de las autoridades de certificación que las entregan a los usuarios y pueden retirarlas en cualquier instante. Como puede observarse, en este sistema el control de la identidad está centralizado, es decir, es una autoridad central la que supervisa y maneja las identidades digitales de los operadores y no los propios usuarios —quienes, en contra de su voluntad, pueden ser despojados de su identidad o sufrir los efectos de una identidad falsa— (Allen, 2016).

En segundo lugar, hay que destacar el modelo de identidad federada. Su objetivo era la creación de una identidad digital que los usuarios pudieran emplear en diferentes entornos virtuales (González Granado, 2023: 16). En este modelo, el control de las identidades correspondía a las múltiples autoridades federadas. Sin embargo, solo se consiguió elaborar una oligarquía, pues la única diferencia con el sistema centralizado es que en este modelo el poder de decisión y control correspondía a unas pocas autoridades (Allen, 2016).

En tercer lugar, se creó el modelo de identidad centrada en cada usuario, es decir, aquel en cuya elaboración se partía de la premisa de que cada individuo tenía el derecho de controlar su propia identidad digital. Desde un punto de vista teórico, esta idea es fundamental para lo que hoy se conoce como identidad auto-soberana. No obstante, desde la óptica práctica, distintas compañías tecnológicas impidieron alcanzar el objetivo de que los usuarios controlasen sus propias identidades digitales y la propiedad final de las identidades continuó siendo de las autoridades encargadas de registrarlas (Allen, 2016).

Finalmente, emerge el denominado modelo de identidad digital autosoberana, que propone que cada usuario disponga de una única identidad digital validable en cualquier entorno digital y que cada persona sea la que ejerza el control exclusivo y la gobernanza de la misma (González Granado, 2023: 17).

Para determinar qué modelo está actualmente vigente en España, habrá que recurrir a dos normas: a nivel europeo el Reglamento eIDAS y el Reglamento eIDAS 2 y a nivel estatal la Ley 6/2020, de 11 de noviembre, reguladora de determinados aspectos de los servicios electrónicos de confianza, pues estos cuerpos normativos son los que regulan los sistemas con los que se identifica a las personas en el ámbito digital, los servicios de confianza que permiten su identificación y las instancias que garantizan los datos contenidos en esos servicios.

Por el momento, la legislación europea —los Reglamentos eIDAS— destina la identificación electrónica mediante servicios de confianza a las actuaciones que los usuarios quieran realizar en relación con los servicios públicos a nivel nacional o comunitario[16].

De acuerdo con el artículo 3 del eIDAS, un servicio de confianza es aquel servicio electrónico prestado normalmente a cambio de una remuneración que consiste en: *i)* la creación, verificación y validación de firmas electrónicas, sellos de tiempo electrónicos, sellos electrónicos, servicios de entrega electrónica certificada y certificados relativos a estos servicios; *ii)* la creación, verificación y validación de certificados para la autenticación de sitios web; o *iii)* la preservación de sellos, firmas o certificados electrónicos relativos a estos servicios (Ávila Gonzales 2023: 118).

Por otro lado, encontramos los servicios de confianza cualificados, es decir, los servicios de confianza que, además, cumplen con los requisitos que establece el artículo 21 del eIDAS (Canut Zazurca, 2015: 45).

Así las cosas, tal y como está configurado el sistema, es necesario que un tercero garantice que el instrumento de identificación que se está utilizando contiene efectivamente los datos verdaderos del usuario y que no han sido falsificados. Es decir, la legislación requiere que exista un prestador de servicios que actúe como intermediario para la verificación y validación de la identidad digital.

Los prestadores de servicios de confianza pueden ser cualificados o no[17]. Los no cualificados son aquellas personas físicas o jurídicas que proporcionan todos o alguno de los servicios de confianza que se han mencionado. En cambio, los prestadores cualificados son aquellos que han sido calificados como tales por parte del organismo de supervisión, previa verificación de cumplimiento de las condiciones establecidas en el artículo 24 del eIDAS y de los servicios de confianza cualificados (Canut Zazurca, 2015: 45-47)[18].

Como puede observarse, la identidad digital es gestionada por el sector de los prestadores de servicios de confianza. Este sector está formado por las personas físicas o jurídicas que tienen bajo su control los datos de la identidad de los usuarios (Rodríguez Illaraz y Palomo Zurdo, 2023: 378) y que, en consecuencia, pueden revocar o suspender los servicios de confianza[19].

Por lo tanto, hoy en día nos encontramos ante un sistema centralizado donde la gestión y control de la identidad digital queda bajo la supervisión y verificación de una autoridad.

Dado que, como se ha dicho, los servicios de confianza regulados por eIDAS están destinados a hacer posible una interacción fehaciente con los servicios públicos locales y comunitarios, en 2021 surgió la propuesta del eIDAS 2[20]. El objetivo del nuevo Reglamento es configurar un cuerpo normativo que regule la identificación digital transfronteriza dentro de la UE (Gallardo Rodríguez, 2023: 1014). Además, con esta nueva normativa se desea extender los efectos de sus previsiones al sector privado[21].

La legislación europea se orienta a cubrir las necesidades de identidad digital en las transacciones que realizan los usuarios con los organismos públicos. Sin embargo, parece que la intención del legislador es que estos efectos se extiendan al sector privado y los usuarios pueda operar bajo una identidad digital única por cada usuario.

Por lo que respecta a la identidad digital, el eIDAS 2 persigue la creación de una cartera de identidad digital europea que se implantará a través de las tecnologías descentralizadas

y de 5G (Rodríguez Illaraz y Palomo Zurdo, 2023: 364). Para poder implantar este monedero digital que recoge la identidad de un usuario concreto, es necesario elaborar un identificador descentralizado (denominado DID) que, en sí mismo, no es una identidad, sino una serie alfanumérica única y aleatoria que estará bajo el control del internauta (Llaneza González, 2021: 84).

Uno de los rasgos distintivos de un DID es que para configurarlo se utiliza la tecnología de registros distribuidos (DLT) —por ejemplo, *blockchain*—; es decir, para implantar esta cartera de identidad digital no sería necesario el modelo centralizado que existe actualmente. De esta forma, se permite la aplicación de una suerte de esquema de clave pública descentralizada (DPKI), en contraposición a los sistemas clásicos de infraestructura de clave pública (PKI), que normalmente se apoyan en la centralización de la función de emisión bajo la dirección de un prestador (Alamillo, 2019: 3).

Aun así, la propuesta eIDAS 2 afirma que «[…] el Reglamento propuesto generará costes financieros y administrativos que deberán ser asumidos por los Estados miembros como emisores de las carteras de identidad digital europea, así como por los prestadores de servicios de confianza y en línea». Es decir, el eIDAS2 continúa relacionando el poder de creación, expedición, gestión y verificación con la figura de los Estados y los prestadores de servicios de confianza, lo que, en consecuencia, evidencia los deseos de la UE de mantener un sistema centralizado, aunque la propuesta se aproxima al modelo de identidad digital autosoberana[22].

En resumen, el proyecto pretende implantar una identidad digital única a nivel europeo que se encontrará disponible para los ciudadanos y residentes de la UE que requieran identificarse o confirmar una información personal determinada y que podrá aprovecharse para acceder a servicios tanto públicos como privados a través de una cartera de identidad digital personal e individual en la que, mediante los datos de identificación básicos de una persona (como son nombre, apellidos, DNI y fecha de nacimiento), a los que podrán añadirse otros (titulaciones, salud, bancos etc.); en cada caso particular, los usuasior gestionarán su cartera de identidad y decidirán qué datos transferir a cada prestador o proveedor de servicios en línea (González Granado, 2023: 14-15).

Como se ha dicho, la UE traspasa la competencia de emisión de las carteras de identidad digital europea a los Estados miembros. De esta forma, surge la cuestión de cómo va a responder España.

Hasta ahora, en virtud de la disposición adicional sexta del artículo 3 del Real Decreto-ley 14/2019, de 31 de octubre, por el que se adoptan medidas urgentes por razones de seguridad pública en materia de administración digital, contratación del sector público y telecomunicaciones, no se permitían en las relaciones con los servicios públicos los sistemas de identificación o de firma basados en las tecnologías de registros distribuidos. Es más, como indica el segundo apartado de la disposición, solo podrán ser utilizados si lo prevé la legislación y siempre y cuando la Administración General del Estado actúe como intermediaria para garantizar la seguridad pública.

El precepto mencionado mantiene que no serán admisibles «[…] en tanto que no sean objeto de regulación específica por el Estado en el marco del Derecho de la Unión Europea».

Con la llegada del eIDAS 2, se cumple dicha previsión, y España, mediante la Resolución de 6 de julio de 2023, de la Secretaría de Estado de Digitalización e Inteligencia Artificial, por la que se publica el Acuerdo del Consejo de Ministros de 27 de junio de 2023, por el que se determinan los supuestos de validez de sistemas de identificación y firma electrónica en la Administración del Estado cuya verificación se lleve a cabo por medio de un sistema de tecnología de registro distribuido, pasa a

> «[…] considerar válido un sistema de identificación y firma de los interesados por medio de una credencial incorporada a la Cartera digital cuya verificación se lleve a cabo por medio de un sistema de tecnología de registro distribuido basado en la Infraestructura Europea de Servicios de Blockchain».

Como se explicará más abajo, *blockchain* es un sistema descentralizado[23] capaz de garantizar la confianza entre los participantes sin necesidad de que una autoridad central actúe como intermediario[24]. Sin embargo, el segundo precepto de la Resolución mencionada afirma que «[…] la Administración General del Estado actuará como autoridad intermedia que ejercerá las funciones que corresponda para garantizar la seguridad pública con relación a los sistemas que se refiere este Acuerdo». De esta forma, se distorsiona la esencia de *blockchain* y se pierde uno de sus caracteres fundamentales que hacen única a esta tecnología: la desintermediación.

Realizado el análisis de la situación jurídica en la que se encuentra actualmente la identidad digital y de las normas encaminadas a paliar los problemas de identidad, persiste la duda de qué ocurre con el resto de los internautas que se encuentran fuera del acervo legislativo de la UE y que tienen que identificarse para acceder a determinados servicios electrónicos.

Internet es un sistema que tiene un alcance global, es decir, no tiene fronteras (Andrade Salazar, Contreras Cedeño, Gómez Tuarez, Cuzco Piedra y Sinchiguano Moreira, 2023: 951). El Derecho surge de la persona. Por consiguiente, este concepto es el fundamento del Derecho global, y se ha impuesto a la idea, tan difundida actualmente, de un Derecho eminentemente legal que emana de disposiciones jurídicas controladas por un Estado o grupo de Estados a través de una comunidad, por ejemplo la UE (Domingo, Ortega, Rodríguez-Antolín y Zambrana, 2006:128).

Ya se ha dicho que la identidad digital hace referencia a los caracteres esenciales de la persona que hacen que pueda ser identificable en del mundo virtual. A este respecto, la Agenda de Naciones Unidas, mediante su Proyecto de resolución remitido a la cumbre de las Naciones Unidas para la aprobación de la Agenda para el desarrollo después de 2015 por la Asamblea General en su sexagésimo noveno período de sesiones, obliga a los países a proporcionar antes del año 2030 una identidad legal para todos los ciudadanos (*ex* objetivo 16.9). Esta cuestión es muy importante porque: *i)* la identidad es un concepto que no tiene un significado global ni es un término reconocido tradicionalmente en muchos países; y

ii) un organismo internacional como la ONU indica que, según el Derecho internacional, debe existir un derecho individual a la identidad y que, por consiguiente, los Estados tendrán que reconocer en sus ordenamientos jurídicos la identidad digital como derecho global (Gallardo Rodríguez, 2023: 1013-1014).

De esta forma y a la vista de lo expuesto, nos encontramos ante un derecho que debe ser reconocido internacionalmente y que se ejerce en una red mundial sin fronteras, por lo que de poco sirve una regulación estatal o europao.

Con ello, ¿qué posibilidades tenemos actualmente para garantizar el derecho a la identidad digital en una red que no conoce de fronteras? En efecto, anteriormente se ha hecho alusión a la tecnología que puede hacer posible esto: *blockchain*, otro sistema que no conoce de fronteras porque su alcance es transnacional[25].

4. IDENTIDAD DIGITAL ÚNICA A NIVEL INTERNACIONAL CON *BLOCKCHAIN*

Actualmente, pertenecemos a la denominada sociedad digital, en la que el papel de los Estados se ha reducido claramente debido al carácter global de Internet (De Salamanca Rodríguez, 2016: 37).

A la luz de esta consideración, puede colegirse que las dimensiones de Internet escapan de las regulaciones locales y comunitaria, y que es necesario buscar una alternativa que posibilite garantizar la identidad digital de los usuarios a nivel mundial[26].

La *blockchain* puede ayudarnos a registrar cada una de las identidades digitales de las personas y, como veremos a continuación, se puede utilizar como tecnología que permita al usuario identificarse dentro de los espacios digitales[27].

Cuando nos enfrentamos al concepto de *blockchain*, debemos tener presente que existen muchas formas de definir esta tecnología (Alvarado Bayo y Supo Calderón, 2021: 350). Esto se debe a que el alcance funcional de *blockchain* es muy amplio[28]. Por ello, las definiciones de esta tecnología normalmente centran su atención en las múltiples aplicaciones a las que se puede destinar (Hierro Viétez, 2021: 300).

A la hora de analizar *blockchain* como un sistema que nos permita identificarnos en Internet deberemos entender esta tecnología como un libro digital compartido formado por bloques conectados y archivados en una red distribuida, descentralizada y protegida a través de criptografía que nos proporciona un depósito de información incorruptible e inmutable (Pacheco Jiménez, 2019: 63).

Además, algunos autores proponen una definición que hace referencia a la capacidad de esta tecnología para identificar a las personas dentro de los espacios digitales. En este sentido, la *blockchain* puede ser entendida como un «[…] protocolo de verificación de identidad descentralizado emitido por un proveedor de servicios que no es una autoridad

estatal, capaz de verificar la identidad de un participante y luego publicar una firma de identidad» (Lucas durán y García Martínez, 2019: 180).

Los bloques que conforman la *blockchain* contienen información. Esta información refleja los datos de las transacciones de cualquier índole, es decir, los eslabones de la cadena pueden contener datos de cualquier tipo: valores, bienes, dinero, propiedades, votos (Beck y Müller-Bloch, 201: 5390), pero también, los datos personales que conforman la identidad digital de las personas.

Además, la tecnología *blockchain* posee una serie de características que la hacen idónea para ser utilizada como sistema de identificación dentro del ámbito digital. A continuación, se expondrán los rasgos más importantes que la conforman como herramienta apropiada para registrar la identidad digital y, por ende, para identificar a los usuarios dentro del entorno virtual.

La información que contiene *blockchain* es inmutable, es decir, todas las transacciones que se almacenan y registran en los bloques no pueden manipularse ni eliminarse. En caso de cambio, el *software* que se está introducido en los bloques es capaz de registrar de forma automática en un nuevo eslabón la nueva transacción sin variar el bloque anterior, facilitando que cualquier usuario pueda observar si la información ha variado o no (Charles, Emrouznejad y Gherman, 2023: 10).

Junto con la inmutabilidad, *blockchain* es una tecnología que aporta una enorme seguridad a los usuarios de la red. Los bloques que conforman la cadena se ordenan por orden cronológico y poseen un código alfanumérico denominado *hash* que corresponde al eslabón que les precede. Gracias a este código, todos los bloques se encuentran verificados con el bloque que los creó y, por lo tanto, solo se introducen y distribuyen los bloques que contengan ese código válido, eliminando las posibilidades de que se registren bloques cuya información no corresponda con el código de la red, minimizando la posibilidad de fraude, suprimiendo la pérdida de datos y conformando un sistema totalmente trazable en el que verificar que la información es correcta (Yahari Navarro, 2017: 7).

Dentro de *blockchain* no existe una autoridad central que coordine y controle la red. La descentralización es tal que se elimina cualquier intermediario y/o autoridad central. Cada nodo tiene la misma copia del registro para mantenerlo actualizado de acuerdo con las normas del protocolo de consenso que se hayan establecido (Alvarado Bayo y Supo Calderón, 2021: 352).

El sistema *blockchain* se caracteriza también por su transparencia, es decir, los participantes de la red están capacitados para acceder a la información y verificarla mediante la cadena de bloques que contiene la información de las transacciones (Corredor Higuera y Díaz Guzmán, 2018: 410).

La *blockchain* es un sistema que está distribuido entre todos los participantes de la red. Cada ordenador (también denominado nodo) posee una copia idéntica del libro digital, lo que garantiza que los datos contenidos en los bloques sean más fácilmente identificables y verificables por el resto de los usuarios (Charles, Emrouznejad y Gherman, 2023: 10).

Habida cuenta de las características de la *blockchain* y de sus capacidades como tecnología, en el siguiente apartado analizaremos cómo podrá utilizarse este sistema como mecanismo en el que se encuentren registradas las identidades digitales de los usuarios y, por ende, que demuestre que las actividades u operaciones que realiza un usuario corresponde a este y no a otra que le esté suplantando y que acredite que el usuario no utilicza una identidad falsa que no corresponda a ningún sujeto o que emplee una identidad con la que no se le pueda trazar.

La identidad digital es compleja, multifuncional y de gran relevancia. Actualmente, los usuarios tienden a administrar múltiples versiones de uno mismo que se hacen visibles en los diferentes entornos virtuales en los que operan las personas. Este hecho nos conduce a un nuevo desafío mundial: las posibles transgresiones de datos personales en línea y los sistemas de identificación vigentes (Merchán Murillo, 2021: 187).

Uno de los problemas que se presentan Internet es la certificación de la identidad de los usuarios. Hasta ahora, ninguna persona que operaba dentro de la red poseía una identidad digital única y consolidada. Sin embargo, esto puede cambiar con la tecnología *blockchain* (Colle, 2018: 4)[29].

A la vista de la capacidad de *blockchain* para servir como registro de identidad digital y, por consiguiente, como sistema de identificación dentro de los entornos digitales, las Naciones Unidas junto con la compañía Microsoft y la alianza Hyperledger tomaron la iniciativa de desarrollar un sistema capaz de proporcionar identidades digitales a los usuarios mediante tecnología *blockchain* (Sundararajan, 2021).

Como vemos, la idea de emplear *blockchain* como sistema de registro de identidades digitales y de identificación dentro de Internet ya navega por la mente de las personas. Sin embargo, resulta erróneo su encuadre, pues, como se ha reiterado, Internet es una herramienta global que puede ser utilizada desde cualquier parte del mundo y por cualquier persona.

Con el fin de que el lector entienda la funcionalidad de *blockchain* como sistema certificador de identidad digital, es preciso analizar el ya mencionado concepto de identidad digital autosoberana (González Grandado, 2023: 16).

A simple vista, con la identidad digital autosoberana, a la hora de identificarse dentro del espacio digital los usuarios podrán acceder seleccionando su propia y única identidad digital, que estará bajo su propio control y gobierno. Con ella, los servicios web otorgarían su acceso prácticamente de forma automática, evitando que los usuarios tengan que cumplimentar continuamente formularios para introducir sus datos de identidad, los cuales pueden estar viciados en cada servicio al que quieran acceder individualmente (Muñoz Moruno, 2020: 6)[30].

Ahora bien, para que esta identidad pueda estar controlada y gestionada por cada uno de los usuarios sin que una autoridad la gobierne o sea capaz de controlarla, es necesario la implementación de la tecnología *blockchain*[31].

La identidad digital autosoberana no estará almacenada dentro de cada uno de los proveedores de servicios que existen en el entorno virtual, sino que dependerá directamente de *blockchain*. Como se ha visto, esta tecnología es capaz de descentralizar el panorama digital y contribuir a que exista una única identidad que sea interoperable, es decir, creada por el usuario y utilizable por igual ante cualquier proveedor de servicios (Gallardo Rodríguez, 2023: 1016).

Tal es la revolución introducida por este modelo que llevó a que algunos países comenzaran a emitir normas técnicas de configuración de la tecnología Blockchain. Así, el 20 de diciembre de 2020, en España, la Asociación Española de Normalización, UNE, publicó la Norma UNE 71307-1 titulada *«Tecnologías Habilitadoras Digitales. Modelo de Gestión de Identidades Descentralizadas sobre* Blockchain y otras Tecnologías de Registros Distribuidos. Parte 1: Marco de referencia», donde determina:

> «Un marco de referencia genérico para la emisión, administración y uso descentralizados de aquellos atributos que faciliten la caracterización (identificación) de individuos u organizaciones, permitiendo a estos últimos crear y controlar su propia identidad digital de forma autogestionada, sin la necesidad de recurrir a autoridades centralizadas»[32].

El objetivo principal del sistema de identidad digital autosoberana dentro de *blockchain* es unificar las credenciales y los datos personales de los usuarios dentro de un sistema legal y totalmente válido. En este entorno, el usuario será capaz de registrar sus datos y credenciales para que, una vez introducida la información, los proveedores de servicios puedan consultarla y verificarla a fin de permitir el acceso a sus entornos virtuales o efectuar transacciones (Santos-Cabaleiro, 2022: 30).

Así las cosas, el desarrollo de la identidad digital mediante *blockchain* permite implementar el concepto de identidad autosoberana descentralizada sin la intermediación de entidades, autoridades o terceros, identidad que está compuesta por testimonios, afirmaciones y evidencias, técnicamente llamadas credenciales verificables, autenticadas por su emisor y comprobadas a través de mecanismos criptográficos. De esta forma, la red *blockchain* almacenará los datos de identidad de cada usuario, el emisor, la fecha, el receptor, el destino y uso de esta información sin que exista la necesidad de que una autoridad se encargue de acreditarla o transmitirla (Madrazo Aguirre, 2020: 25).

Actualmente nos encontramos ante sistemas centralizados en los que pueden utilizarse identidades fraudulentas. La identidad digital está fragmentada y dividida entre los diferentes espacios virtuales que frecuentan los usuarios. Adicionalmente, la conexión entre las identidades digitales y las físicas es escasa, lo que facilita la creación y utilización identidades falsas. Con el uso de *blockchain* y de la criptografía pueden crearse sistemas de gestión de identidad basados en identificadores descentralizados protegidos por una clave privada esté bajo control de cada usuario para solucionar este entramado de problemas (Fiaño Rodríguez, 2022: 17).

Asimismo, el uso de *blockchain* para elaborar sistemas de gestión de identidad descentralizados comportaría la eliminación de los sistemas centralizados, acrecentería la confianza en los entornos virtuales, garantizaría la integridad de los datos personales de los

usuarios, eliminaría los intermediarios y traspasaría el control y gestión de los datos e identidades digitales a los propios usuarios siempre y cuando mantengan el dominio de las claves criptográficas que les dan acceso a ellos (Fiaño Rodríguez, 2022: 17).

A la vista de la posibilidad de crear un sistema de alcance internacional en el que cada usuario tenga en su poder su propia identidad digital y sea capaz de gestionarla y utilizarla con libertad dentro de los entornos virtuales, se plantea la cuestión de a quién corresponde acreditar que la información contenida en la *blockchain* es veraz, corresponde a la identidad real del usuario y no se ha manipulado a efectos de actuar fraudulentamente en el ámbito digital.

Para que la identidad en *blockchain* sea efectiva es necesario que exista un punto de conexión con el mundo físico, es decir, resulta imprescindible que alguien dé fe de que la identidad que se encuentra registrada en *blockchain* coincide con la identidad real del usuario, tarea que pueden llevar a cabo los notarios (en caso de España) o los fedatarios públicos de los distintos países del mundo (Puig Pascual, 2018: 4)[33].

Con todo, aunque esta tecnología fue creada pensando en las criptomonedas, se han ido descubriendo diferentes utilidades para diversos sectores. Actualmente, se utiliza en gran variedad de aplicaciones: pagos globales, compartición y registro de música, trazabilidad de ventas y cadena logística, sistemas de voto, etc. Como puede verse, *blockchain* permite registrar cualquier información y, dado su potencial, se ha dicho que puede llegar a ser la base de una nueva Internet (Colle, 2018: 3).

En definitiva, para que la identidad digital se convierta en una realidad universal, es necesario un protocolo estándar aceptado por todos los países del mundo que tenga como fin registrar y procesar todos los datos de las personas que se conecten a Internet (Colle, 2018: 7). Como se ha visto, actualmente la mejor tecnología que puede garantizar la identidad digital a nivel global es *blockchain* debido a las características que la conforman.

No debe olvidarse que, para implantar esta tecnología como sistema de identificación digital, debe realizarse una revisión normativa de los diferentes países y adaptarla a un marco estándar[34], común e internacional. En particular, podemos señalar el caso de la protección de datos dentro del ordenamiento jurídico de la UE. Para implantar la identidad digital descentralizada será necesario revisar, entre otras normas, el Reglamento (UE) 2016/679 Del Parlamento Europeo y del Consejo de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos, en adelante RGPD), pues su diseño se efectuó de acuerdo con los sistemas centralizados y no con los descentralizados, por lo que, por ejemplo, la figura del encargado del tratamiento no encaja dentro de los modelos descentralizados que emplea *blockchain* (Fiaño Rodríguez, 2022: 18).

Además, como se ha indicado, una de las características que posee *blockchain* y que permiten catalogarla como un sistema garante de identidad digital es la inmutabilidad de la información de sus bloques. Sin embargo, la imposibilidad de modificar la información que contiene el libro distribuido choca directamente con el derecho al olvido regulado en

el artículo 17 del RGPD. Este derecho es un aspecto fundamental de la soberanía del ciudadano sobre su identidad y la relación de esta con las entidades privadas o públicas. El citado precepto reconoce el derecho de los usuarios a suprimir sus errores, es decir, cualquier internauta puede ejercer su derecho a eliminar cualquier aspecto de su identidad para que sus datos no se mantengan indefinidamente en la red y puedan seguir siendo empleados por terceros (Fiaño Rodríguez, 2022: 18). Por tanto, es bnecesario la adaptación de ciertas disposiciones para que el sistema *blockchain* de identidad digital internacional surta todos sus efectos y se ajuste a las disposiciones locales[35].

5. CONCLUSIONES

Hasta hace unos años, las personas solo tenían que ser identificadas mediante una identidad física conformada por una serie de características y datos individuales que distinguían a unos individuos de otros[36].

Con la aparición y posterior evolución de Internet, las personas comienzan a navegar dentro de la red y actúan prácticamente igual que en el mundo analógico, es decir, interactúan con otros sujetos, realizan compras, poseen perfiles en redes sociales, consumen material audiovisual, juegan a videojuegos en línea, etc.

A medida que los usuarios interactúan en la red como en el mundo real, se torna necesaria la implantación de una identidad digital única que permita identificar e individualizar a los internautas. La creación de una identidad digital única ayuda a prevenir los riesgos del anonimato en Internet y facilita la realización de operaciones en línea, garantizando la responsabilidad en caso de que surjan consecuencias legales.

Hoy en día, los usuarios disponen de múltiples identidades digitales creadas por ellos mismos. ¿Quién no tiene varias cuentas de correo electrónico o distintos perfiles dentro de las diversas redes sociales que existen? Internet permite a los usuarios tener múltiples identidades digitales. Asimismo, los usuarios pueden hacerse pasar por otras personas, ya que son ellos quienes crean los perfiles dentro de las redes.

A todo ello hay que sumar el acceso generalizado a Internet que se ha alcanzado a lo largo de los últimos años. Es extraño encontrar a alguien que no pueda acceder a la red, pues disponemos de ordenadores y otros dispositivos como teléfonos inteligentes que tienen acceso constante a Internet.

A la vista de tal situación, es necesario que los internautas dispongan de una única identidad digital que les individualice del resto y, en consecuencia, puedan ser identificados a la hora de investigar quién «anda detrás» de un determinado perfil o quién ha podido ser el responsable de determinadas actuaciones ilícitas en la red.

La UE propone como solución la implantación de una cartera única digital que recoja los datos esenciales que hacen posible la identificación fehaciente de una persona en Internet. Este mecanismo de garantía de la identidad digital se propone para que los Estados

miembros lo implanten con el fin de identificar dentro en la red a los individuos cuya residencia habitual se encuentre dentro del territorio de la Unión o a los ciudadanos que pertenezcan a ella.

Ahora bien, Internet no se circunscribe a territorios determinados, sino que es global y no tiene fronteras. De poco sirve que un determinado conjunto de personas sí posea una identidad digital única cuando en otras partes del mundo los internautas pueden continuar realizando transacciones y actuaciones en la red con identidades falsas o que no identifiquen verdaderamente a la persona que está detrás.

Además, el concepto de identidad digital sigue en constante evolución: todavía no existe una definición legal unificada y global, su regulación internacional es igualmente incierta y, aunque existe predisposición para regularla, aún queda un largo camino por recorrer.

A la vista de todo ello, resulta pertinente la implantación de algún sistema que, mientras se reconoce y regula internacionalmente el concepto de identidad digital, dé respuesta a la inseguridad jurídica que supone actuar en Internet sin una identidad clara y verdadera que permita identificar fiablemente a los usuarios. Este sistema puede ser *blockchain*.

Actualmente, la forma de administrar la identidad digital es centralizada, es decir, la gestión y supervisión de las distintas identidades está bajo el control de los proveedores de servicios de la red. Con *blockchain* este sistema puede evolucionar hacia una identidad digital única descentralizada controlada únicamente por los usuarios, que podrán utilizarla en los sitios que deseen sin que un tercero aporte confianza o controle sus datos.

Las características de la tecnología *blockchain* (inmutabilidad, seguridad, descentralización, etc.) ligadas al carácter trasnacional del libro distribuido que la conforma, hacen que este sistema sea una opción idónea para que en él se encuentren registradas los distintos datos de identidad de la persona y, además, sea el propio usuario quien los controle y decida qué información facilitar a los prestadores de servicios.

Si bien hoy por hoy la descentralización total del sistema es prácticamente imposible porque la información de identidad digital que contiene *blockchain* puede haberse introducido erróneamente o con el objetivo de crear una identidad falsa. De esta forma, será necesaria la figura de un tercero que dé fe de que los datos son veraces y corresponden a la persona que ha introducido dicha información. A través de, por ejemplo, organismos garantes de confianza o de un fedatario público, como en España los notarios, puede resolverse este inconveniente puede resolverse mediante la creación de un sistema de identidad digital internacional, que es lo que realmente interesa a quienes firmamos este artículo y, creemos, al mundo en general.

Como se ha visto, los problemas, incertidumbre y falta de seguridad que encontramos actualmente en la red debido a la falta de una identidad digital única que individualice a los usuarios y permita trazarlos hace necesaria la búsqueda de alternativas mediante las herramientas disponibles en tanto el marco jurídico internacional encuentre una regulación global para la identidad digital y construya un sistema que garantice la identidad digital que todo usuario debe tener en Internet.

En definitiva, con la implantación de una identidad digital única, global y descentralizada a través del uso de *blockchain*, los usuarios podrán controlar sus datos dentro de la red, facilitando la información que deseen a los distintos proveedores de servicios, se evitará que esos datos queden en manos de terceros que puedan comerciar con ellos, podrá prevenirse la comisión de actuaciones ilícitas —pues los internautas podrán ser identificados— y se aportará seguridad jurídica y confianza a las transacciones mundiales que se realicen en los entornos digitales.

NOTAS

1. *Vid*. Martín Diz (2024: 113).

2. Lavín, Olate y Zambrano (2013: 18) han sostenido que «[…] los seres humanos poseemos una identidad única e invariable». También Rodríguez Galván (2017: 28) señala que «[…] como individuos poseemos una identidad única la cual se debe de proteger».

3. Finocchiaro (2012: 737) afirma que «[…] Internet un sistema potente en el que se pueden asumir diversas identidades. Como expresa la autora es fácil poseer multitud de identidades dentro de las redes sociales, juegos y páginas donde se crean diversos avatares».

4. Batuecas Caletrío (2022: 927-928) ha observado que «[…] la identidad es inherente a la persona y, en este sentido, se reconoce identidad tanto a las personas físicas como a las jurídicas».

5. Ballesteros (2001) lo ha expresado en los siguientes términos: «[…] tener identidad, ser un sujeto, equivale a poder ser juzgado».

6. González Granado, (2023: 14) afirma que «[…] todos los derechos humanos que existen *offline* deben también estar protegidos online». Por su parte, Gallardo Rodríguez (2023) apunta que «[…] es de obligada referencia tratar el reconocimiento legal a nivel europeo por medio del Reglamento eIDAS, así como a nivel nacional en España, en la Carta de Derechos Digitales, al reconocer por primera vez el "Derecho a la identidad en el entorno digital"».

7. Según Gallardo Rodríguez (2023: 1010), «[…] desde la irrupción de Internet, la identidad física evoluciona a una identidad digital o identidad 2.0, a través de las acciones que realizamos en Internet».

8. Benach y Pueyo (2013: 75) han afirmado que «[…] el correo electrónico, los formularios, la imagen, la geolocalización, los avatares, direcciones y nicknames constituyen elementos muy importantes en la configuración de nuestra identidad».

9. Pues, como indica Batuecas Caletrío (2022), «[…] los datos existentes en Internet que deberán tenerse en cuenta para conformar la identidad digital serán […] datos "oficiales" que existan de la persona (entendiendo por tales los así reconocidos por el ordenamiento jurídico: nombre, apellidos, filiación, número del DNI, fecha y lugar de nacimiento, etc.), datos reconocidos auténticamente por la propia persona (ideología, creencias, etc.) (…) y, finalmente, datos que objetivamente pueda probarse que forman parte de la identidad de la persona (p. ej., pertenencia a asociaciones, intervenciones públicas que reflejen su pensamiento, etc.)».

10. En este sentido, el considerando 13 del Reglamento (UE) N.º 910/2014 del Parlamento Europeo y del Consejo de 23 de julio de 2014 relativo a la identificación electrónica y los servicios de confianza

para las transacciones electrónicas en el mercado interior y por la que se deroga la Directiva 1999/93/CE afirma que «[…] los Estados miembros deben seguir siendo libres de utilizar o introducir, a efectos de identificación electrónica, medios de acceder a los servicios en línea. También deben poder decidir si interviene o no el sector privado en la prestación de estos medios».

11. Propuesta de Reglamento del Parlamento Europeo y del Consejo por el que se modifica el Reglamento (UE) n.º 910/2014 en lo que respecta al establecimiento de un marco para una Identidad Digital Europea.

12. *Vid*. Sanmartín (2024).

13. Calderón Palomar (2024) indica que «[…] hecho significativo es que, los menores cuentan antes con su identidad digital que con su Documento Nacional de Identidad».

14. *Vid*. Pérez Gurrea (2012).

15. Por ejemplo, en Facebook la edad mínima para poder registrarse es de 13 años en general y 14 en España: <https://www.facebook.com/help/100532533374396/?helpref=faq_content>. [Consulta: 13/05/2024.]

16. Como han puesto de manifiesto Guerola-Navarro, Oltra Badenes, Gil Gómez y Stratu Strelet (2019: 69), «[…] el Reglamento eIDAS garantiza que las personas y las empresas puedan utilizar sus propias identificaciones electrónicas nacionales para acceder a servicios públicos en línea en otros países de la UE».

17. El Ministerio de Industria y Turismo pone a disposición de los usuarios una página donde poder consultar quiénes son prestadores cualificados y quiénes no. Disponible en: <https://sede.serviciosmin.gob.es/es

-es/firmaelectronica/paginas/Prestadores-de-servicios-electronicos-de-confianza.aspx>. [Consulta: 23/02/2024.]

18. España, a través del Ministerio para la transformación digital y de la función pública recoge un listado accesible para todos los usuarios donde recopila todos los prestadores cualificados de servicios de confianza. Disponible en: <https://sedediatid.mineco.gob.es/Prestadores/TSL/TSL.pdf>. [Consulta: 23/02/2024.]

19. *Vid.* Art. 5 de la Ley 6/2020, de 11 de noviembre, reguladora de determinados aspectos de los servicios electrónicos de confianza.

20. Propuesta de Reglamento del Parlamento Europeo y del Consejo por el que se modifica el Reglamento (UE) n.º 910/2014 en lo que respecta al establecimiento de un Marco para una Identidad Digital Europea.

21. Según el considerando 1 de la Propuesta de Reglamento del Parlamento Europeo y del Consejo por el que se modifica el Reglamento (UE) n.º 910/2014 en lo que respecta al establecimiento de un Marco para una Identidad Digital Europea. Disponible en: <https://eur-lex.europa.eu/resource.html?uri=cellar:5d88943a-c458-11eb-a925-01aa75ed71a1.0018.02/DOC_1&format=PDF>. [Consulta: 14/04/2024.]

22. *Vid.* Ibáñez Jiménez (2018).

23. «Las ventajas señaladas son consecuencia de las dos principales características de esta «tecnología»: ser una base de datos online de carácter descentralizado» (Legerén Molina, 2019: 181).

24. «Esta novedosa tecnología permite eliminar intermediarios, pero garantizando –e incluso aumentando– la seguridad que aquellos proporcionaban» (*ibid.*: 177).

25. Padilla Sánchez (2020) ha explicado que «[…] se trata de un esquema de naturaleza transnacional en el que los partícipes pueden tener acceso a servicios globales desintermediados».

26. «Es importante que las credenciales verificables emitidas en tecnología Blockchain puedan interoperar entre redes, y por ello es necesario establecer unos estándares globales comunes a todas las redes DLT» (Latorre Salvador, 2021: 56).

27. Como indican Lucas Durán y García Martínez (2019) «[…]la identidad digital puede certificarse por una autoridad estatal tanto como por terceros con un sistema de confianza. Con todo ello podemos concluir que una de las claves para controlar las operaciones en el ámbito virtual, […], es la identidad digital y que ésta no está ya exclusivamente en manos de las autoridades, sino que a efectos de poder controlar la identidad […] pueden establecerse sistemas efectivos y eficientes impulsados desde iniciativas privadas».

28. «Todas las características de la tecnología *blockchain* confieren a esta una amplia variedad de usos» (Touriño Peña *et al.*, 2022: 15).

29. *Vid.* Sullivan y Burger (2017).

30. Puig Pascual (2018) sostiene que hay que tener presente que «[…] no solo identidades personales pueden ser certificadas en blockchain, también se pueden representar empresa, propiedades… Yo podría demostrar que soy el administrador único de mi empresa y permitir que esta u otros soportes de operaciones y contratos».

31. *Vid.* Merchán Murillo (2021).

32. UNE (2020).

33. De Salamanca Rodríguez (2016: 37) afirma que «[…] los propios internautas irán fijando las reglas de ese ciberespacio, y creo profundamente que los notarios podemos convertirnos en notarios 3.0 ofreciendo soluciones a los problemas que plantea y que planteará este entorno».

34. Es cierto que ya desde los órganos internacionales se efectúan diferentes estándares internacionales, prenormativos y de facto con el fin de adoptar globalmente la tecnología *blockchain,* sin embargo, queda un largo camino por recorrer. *Vid.* Latorre Salvador (2021).

35. Existen quienes elaboran proyectos *blockchain* en los cuales se puede, a petición de los usuarios, eliminar ciertos datos para garantizar el derecho al olvido de los usuarios. *Vid.* Dorri, Kanhere y Jurdak, (2019).

36. *Vid.* Fernández Sessarego (1997).

BIBLIOGRAFÍA

ALAMILLO, Ignacio (2019): «Uso de los Sistemas de Identidad Auto-Soberana en el Sector Público Español y de la Unión Europea», *Blockchain Intelligence*, marzo, 1-21

ALBIOL-PERARNAU, Marc e Iris ALARCÓN BELMONTE (2024): «Blockchain en salud: transformando la seguridad y la gestión de datos clínicos», *Atencion Primaria,* 56(5).

ALLEN, Christopher (2016): «The Path to Self-Sovereign Identity», *Lifewithalacrity* [en línea] <https://www.lifewithalacrity.com/article/the-path-to-self-soverereign-identity/>. [Consulta: 14/05/2024.]

ALVARADO BAYO, María del Carmen y Daniela SUPO CALDERÓN (2021): «Blockchain y propiedad intelectual: aplicando una tecnología innovadora en la gestión de derechos intangibles», *THEMIS: Revista de Derecho,* 79, 345-357.

ANDRADE SALAZAR, Milton Temistocles, Jessie Nicole CONTRERAS CEDEÑO, Jenniffer Narcisa GÓMEZ TUAREZ, Maylon Elian CUZCO PIEDRA y Jostyn Steveen SINCHIGUANO MOREIRA (2023): «Una exploración segura en la Deep Web», *Código Científico Revista de Investigación,* 4(2), 949-958.

ÁVILA GONZALES, Nadia Paola (2023): *El comercio electrónico en Bolivia: el nuevo horizonte y sus desafíos jurídicos* (Tesis Doctoral), Repositorio de la Universidad de Valencia.

BATUECAS CALETRÍO, Alfredo (2022): «El derecho a la identidad y la identidad digital», *Anuario de derecho civil*, 75(3), 923-986.

BECK, Roman y Christoph MÜLLER-BLOCH (2017): «Blockchain as Radical Innovation: A Framework for Engaging with Distributed Ledgers as Incumbent Organization», *Proceedings of the 50th Hawaii International Conference on System Sciences*.

BENACH, Ernest y Miquel PUEYO (2013): «La vida, el temps, la mort, la memòriai la identitat», *Item: revista de biblioteconomia i documentació*, 57, 71-80.

BENAVENTE MOREDA, Pilar (2013): «Identidad y contexto inmediato de la persona (identidad personal, el nombre de la persona, identidad sexual y su protección)», *Anuario de la Facultad de Derecho de la Universidad Autónoma de Madrid*, 17, 105-162.

CANUT ZAZURCA, Pedro J. (2015): «El prestador cualificado de servicios de confianza – seguridad jurídica en Internet», *PIDCC: Revista em propriedade intelectual direito contêmporaneo,* 9(2), 41-55.

CHARLES, Vincent, Ali EMROUZNEJAD y Tatiana GHERMAN (2023): «A critical analysis of the integration of blockchain and artificial intelligence for supply chain», *Annals of Operations Research*, 327, 1-41.

COLLE, Raymond (2018, 18 de mayo): «La identidad digital en la internet futura con blockchain», *Asociación Chilena de Investigadores en Comunicación*, 1-12.

CORREDOR HIGUERA, Jorge Armando y David DÍAZ GUZMÁN (2018): «Blockchain y mercados financieros: aspectos generales del impacto regulatorio de la aplicación de la tecnología blockchain en los mercados de crédito de América Latina», *Derecho PUCP,* 81, 405-439.

DE SALAMANCA RODRÍGUEZ, Francisco Rosales (2016): «Testamento digital», en R. Oliva León y S. Valero Barceló (coords.), *Testamento ¿Digital?*, España: Juristas con Futuro.

DOMINGO, Rafael, Javier ORTEGA, Benjamín RODRÍGUEZ-ANTOLÍN y Nicolás ZAMBRANA (2006): *Principios de Derecho Global.* Navarra: Thomson-Aranzadi.

FERNÁNDEZ BURGUEÑO, Pablo (2012): «Aspectos jurídicos de la identidad digital y la reputación online», *Revista de Estrategias, Tendencias e Innovación en Comunicación,* 3, 125-142.

FIAÑO RODRÍGUEZ, Jacobo (2022): *Sistema de Identidad Digital Soberana y Descentralizada basada en Blockchain* (Trabajo de Fin de Grado), Repositorio Univeridade Da Coruña.

FLAMINI, Andrea, Giada SCIARETTA, Mario SCURO, Amir SHARIF, Alessandro TOMASI y Silvio RANISE (2024): «On Cryptographic Mechanisms for the Selective Disclosure of Verifiable Credentials», *arXiv preprint*.

GALLARDO RODRÍGUEZ, Almudena (2023): «Identidad digital y responsabilidad civil de las plataformas digitales: de las redes sociales al metaverso», *Actualidad jurídica iberoamericana,* 18, 1008-1033.

GETE-ALONSO Y CALERA, María del Carmen (2018): «La inscripción de nacimiento en la ley 20/2011. Entre el derecho a la identidad de la persona y la reserva de la maternidad», *Revista de Derecho Civil,* 5(1), 1-54.

GONZÁLEZ GRANADO, Javier (2023): *De la identidad a la identidad digital soberana* [en línea] <https://tallerdederechos.com/de-la-identidad-a-la-identidad-digital-soberana/>. [Consulta: 12/05/2024.]

HIERRO VIÉTEZ, Gonzalo (2021): «Introducción al Blockchain, los contratos inteligentes y su relación con el arbitraje», *THĒMIS-Revista de Derecho*, 79, 299-309.

IBÁÑEZ JIMÉNEZ, Javier Wenceslao (2018): *Derecho de Blockchain,* Navarra: Aranzadi.

LLANEZA GONZÁLEZ, Paloma (2021): *Identidad digital, actualizado a la Orden ETD/465/2021, de 6 de mayo (sobre métodos de identificación remota) y a la propuesta de Reglamento eIDAS2*, Madrid: Wolters Kluwer.
LÓPEZ-MEDEL BÁSCONES, Manuel (2024): «La contemporaneidad del derecho digital y de los derechos fundamentales», en F. J. Santamaría Ramos (dir.), *Derechos Digitales*, Valencia: Tirant Lo Blanch.
LUCAS DURÁN, Manuel (dir.) (2019): *Residencia fiscal: problemática y cuestiones actuales*, Documentos de Trabajo del Instituto de Estudios Fiscales, 6/2019.
MADRAZO AGUIRRE, Teresa Juana (2020): *Identidad digital soberana y tecnología Blockchain. Modelo de negocio y plan de marketing de la start-up «LinKple»* (Trabajo de Fin de Grado), Repositorio de la Universidad Pontificia Comillas.
MARTÍNEZ CALVO, Javier (2020): «El derecho de rectificación ante informaciones falsas o inexactas, con especial mención a las publicadas en Internet/The reply right against false or inexact information, with particular reference to information published on the Internet», *Revista de Derecho civil,* 7(4), 137-181.
MERCHÁN MURILLO, Antonio (2021): «Identidad digital Blockchain e Inteligencia Artificial: aspectos jurídicos de presente y futuro a debate», *Ius et Scientia,* 7(1), 183-203.
— (2022): «La identidad digital en la contratación electrónica: una mirada desde el derecho internacional privado», *Actualidad jurídica iberoamericana,* 16, 1386-1411.
MUÑOZ MORUNO, Laia (2020): Identidad digital soberana (Trabajo de Fin de Grado), *Repositorio de la Universitat Politècnica de Catalunya*.
PACHECO JIMÉNEZ, María Nieves (2019): «De la tecnología blockchain a la economía del token», *Derecho PUCP,* 83, 61-87.
PUIG PASCUAL, Álex (2018): «Identidad digital sobre «Blockchain» a nivel nacional», *ICADE Revista de la Facultad de Derecho,* 101, 1-5.
RODRÍGUEZ ILLARAZ, Clara y Ricardo Javier PALOMO ZURDO (2023): «Transparencia, ciberseguridad e identidad digital en el entorno 5G», *Revista española de la transparencia,*18, 359-380.
RUILOBA CASTILLA, Juan Carlos (2006): «La actuación policial frente a los déficits de seguridad de Internet, *IDP: revista de Internet, derecho y política = revista d'Internet, dret i política*, 2, 52-62.
SALVADOR GARCÍA, Miriam (2024): «Derecho de acceso universal a internet. En F. J. Santamaría Ramos (dir.), *Derechos Digitales*, Valencia: Tirant Lo Blanch.
SANTAMARÍA RAMOS, Francisco Javier (2015): «Identidad y reputación digital Visión española de un fenómeno global», *Ambiente Jurídico*, 17, 11-43.
— (2024): «Datos abiertos y reutilización de la información: una mirada europea», *Revista Canaria De Administración Pública*, Extra 0, 37-64.
SANTOS-CABALEIRO, Pablo (2022): *Análisis y prototipado de Identidad Digital Descentralizada basada en Blockchain* (Trabajo de Fin de Grado), Repositorio Univeridade Da Coruña.
SUNDARARAJAN, Sujha (2021): «Microsoft, Hyperledger, UN Join Blockchain Identity Initiative», *Coindesk* [en línea] <https://www.coindesk.com/markets/2018/01/23/microsoft-hyperledger-un-join-blockchain-identity-initiative/>. [Consulta: 23/05/2024.]
YAHARI NAVARRO, Benjamín (2017): «Blockchain y sus aplicaciones», *Universidad Católica Nuestra Señora de La Asunción* [en línea] < https://bit.ly/2rc0iZ9. Fecha de último acceso: 25/08/2018>. [Consulta: 23/03/2024.]

Legislación

Directiva 1999/93/CE del Parlamento Europeo y del Consejo, de 13 de diciembre de 1999, por la que se establece un marco comunitario para la firma electrónica.
Reglamento (UE) Nº. 910/2014 del Parlamento Europeo y del Consejo de 23 de julio de 2014 relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior y por la que se deroga la Directiva 1999/93/CE.

Propuesta de Reglamento del Parlamento Europeo y del Consejo por el que se modifica el Reglamento (UE) n.º 910/2014 en lo que respecta al establecimiento de un Marco para una Identidad Digital Europea.
Ley 6/2020, de 11 de noviembre, reguladora de determinados aspectos de los servicios electrónicos de confianza.
Ley 20/2011, de 21 de julio, del Registro Civil.
Decreto-ley 14/2019, de 31 de octubre, por el que se adoptan medidas urgentes por razones de seguridad pública en materia de administración digital, contratación del sector público y telecomunicaciones.
Resolución de 6 de julio de 2023, de la Secretaría de Estado de Digitalización e Inteligencia Artificial, por la que se publica el Acuerdo del Consejo de Ministros de 27 de junio de 2023, por el que se determinan los supuestos de validez de sistemas de identificación y firma electrónica en la Administración del Estado cuya verificación se lleve a cabo por medio de un sistema de tecnología de registro distribuido.
Norma UNE 71307-1 titulada «Tecnologías Habilitadoras Digitales. Modelo de Gestión de Identidades Descentralizadas sobre Blockchain y otras Tecnologías de Registros Distribuidos. Parte 1: Marco de referencia.

Fecha de recepción: 16 de julio de 2024.
Fecha de aceptación: 20 de octubre de 2024.